Chakra®

システムへ負荷をかけず、
データベース操作をリアルタイムに

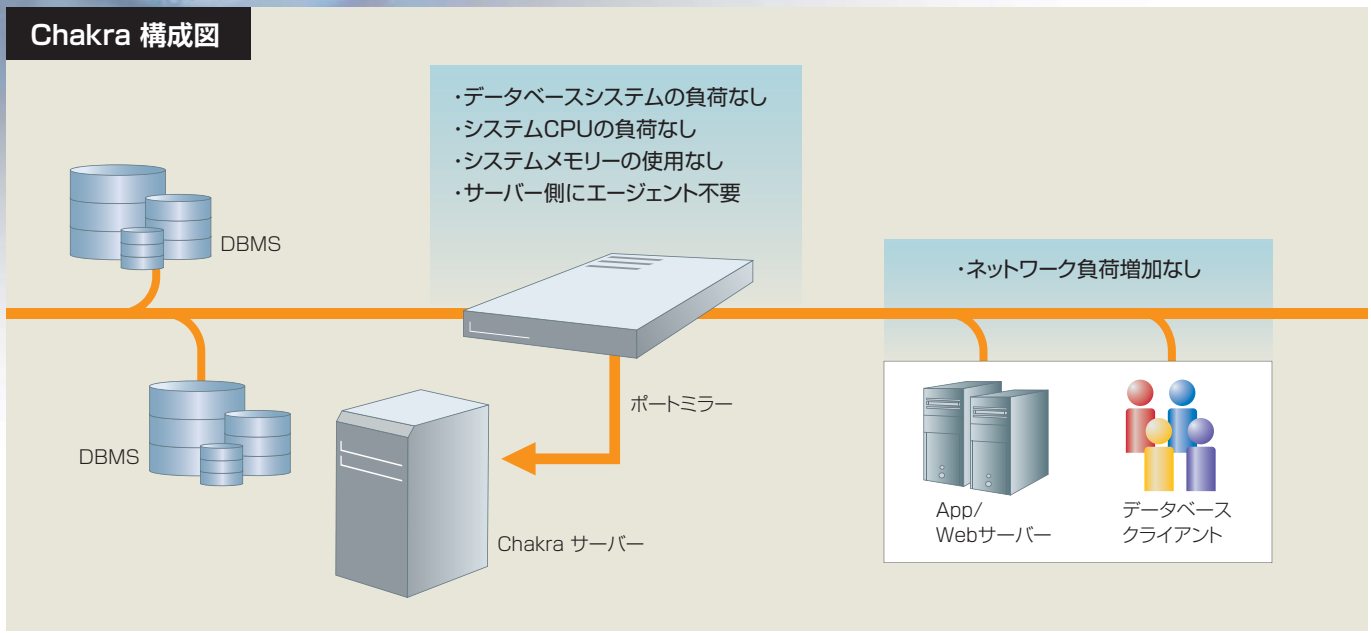
監視・検知・記録・防御

NST
New System Technology

100%の記録を、0%の影響で。

日本版SOX法適用を機に、企業は早急なコンプライアンス対策の必要性に迫られています。
コンプライアンスへの基本は、データベースへのアクセスログを監査証跡として保管すること。
その保管体制は既存のDBシステムに影響を与えずに速やかに確立することが理想的です。
Chakraはすべてのネットワーク経由のアクセスを記録し、
しかもDBシステムへの影響が全くありません。
そしてDBシステムの外側に設置するだけなので簡単に導入でき、
リアルタイム監視、検知、防御、記録が実現します。
貴社のDBは大丈夫でしょうか?DB監視の第三者の眼ともいえるソフトウェアChakraが、
コンプライアンス対策をサポートいたします。

Chakra 構成図



データベースアクセスのセキュリティは万全ですか?

データベースには、企業活動におけるもっとも重要なデータが格納されています。そのデータベースに対するセキュリティは万全でしょうか?ファイアウォールはもちろん、暗号化をおこなっても情報漏洩、情報破壊は防げません。なぜなら、データベースにアクセスできる正規のユーザーが不正を行うケースが非常に多いからです。

Chakraは、データベースアクセスを100%監視。

Chakraは、ネットワーク上を流れているデータベースアクセスのパケットをキャプチャし、プロトコルを解析します。これによって、データベースをアクセスするすべての操作について、何時、誰が、何処から、何をしたのか、何件取得したのかを、リアルタイムに直接把握し、モニターに表示し、予め設定してあるアラートを発生します。データベースに対する更新処理だけでなく、SELECT文、CREATE文、GRANT文やストアドプロシジャーも監視・記録します。

主な監視対象項目

- DBアカウント名
- クライアントのIPアドレス
- クライアントの端末名
- アプリケーション名
- 平均応答時間
- SQLテキスト
- 応答時間
- 結果行数
- バインド変数値
- TELNET/FTPのコマンド など・・・

データベースシステムへの影響が心配ですか?

データベースシステムにエージェントを導入したり、周期的にデータ検索を行うようなシステムでは、データベースシステムに対する負荷やシステム運用時の作業を無視できません。また、DBMSに付随する監査記録機能を利用する場合、完全な記録をとると負荷が30%以上増えるといわれています。そして監査記録の場合は、DBAが作業しますが、DBAは監視対象者なので、セキュリティの観点からは、好ましくありません。

Chakraは、データベースシステムに全く影響を与えません。

Chakraは、ネットワーク上を流れているデータベースアクセスのパケットをキャプチャし、解析することで、データベースを監視します。このため、監視対象のデータベースシステムには、なんら影響を与えません。データベースシステムにエージェントを導入する必要はなく、また、データベースに接続する必要もありません。

説明責任は果たせますか?

不正アクセスが発生した場合、何時、誰がどういう操作を行ったのか、漏洩した情報の範囲は、どこまでなのかを正確に把握できますか?

Chakraは、データベース操作を100%記録。

Chakraでは、ネットワーク上を流れているデータベースアクセスのパケットをキャプチャし、プロトコルを解析します。解析した内容はログとして記録し、後から検証することができます。また、特定アプリケーションについてや、特定時間帯のみをログとして記録することも可能です。データベースサーバーに対するリモートアクセス(TELNET/FTPなど)についても操作内容をログとして記録します。さらに、条件を指定して出力結果そのものをログすることも可能です。また、さまざまな条件を指定してデータベースアクセスについてのレポートやアラート発生状況のレポートを出力することができます。

データベースへのローカルアクセスも監視・検知・防御・記録できます。

未然に不正アクセスを防げますか?

データベースへの不正なアクセスを検知した場合、ただちに処置を行い、情報漏洩を未然に防ぐことができますか?不正なアクセスを検知した際、オペレーターに通知して、オペレーターが原因を調べ、その後処置を行ったのでは、間に合いません。

Chakraは、不正なアクセスをリアルタイムに遮断。

Chakraは、アラート発生時に、その原因となった操作を行っているセッションを破棄することが出来ます。

アラート発生時のアクション

メールにて通知
オペレーターに通知
任意のプログラムを起動
アラートの発生元のセッションを破棄

豊富な実績を誇るChakra

- 数多くの大手企業に選ばれた「信頼」と「実績」。
- 金融、通信、製造、流通、運輸、建設など様々な業種／業態での豊富な導入実績。
- 個人情報、機密情報などへの多彩なデータアクセスログを
  コンプライアンス対策の基本として保管、監査証跡として活用される豊富な事例。

主な仕様

DBアクセスを監視	100%(ローカルアクセスを含む)
アクセスを遮断	可能
DBMSの負荷	0%
データ収集方法	ネットワーク上のパケット
ロギング	すべてのデータベースアクセス
権限変更	監視・検知・防御・記録
スキーマ変更	監視・検知・防御・記録
データ変更	監視・検知・防御・記録
データ検索(SELECT)	監視・検知・防御・記録
ストアドプロシジャー	監視・検知・防御・記録
DBユーザ名	監視・検知・防御・記録
IPアドレス	監視・検知・防御・記録
アプリケーション名	監視・検知・防御・記録
使用端末名	監視・検知・防御・記録

使用時刻	監視・検知・防御・記録
SQL テキスト	監視・検知・防御・記録
応答時間	監視・検知・防御・記録
出力行数	監視・検知・防御・記録
セッション平均応答時間	監視・検知・防御・記録
SQLバインド変数値	監視・記録
Telnet/R-コマンド	監視・検知・記録
FTPコマンド	監視・検知・記録
リアルタイムに警報	可能
非承認ツール	アクセスを遮断可能
警報の条件設定	時間帯、ユーザ名、IPアドレス、端末名、 アプリケーション名、SQL文中の表名、 応答時間、出力行数、など
警報時のアクション	メール送信、オペレータへの通知 プログラム起動、セッション破棄

対応DBMSとプラットフォーム

対応DBMS	Oracle7.3.4, 8.0, 8i, 9i, 9iR2, 10g, 10gR2, 11g, 11gR2 DB2 UDB for Linux / Windows / Unix V6, V7, V8, V9, V9.5 MS SQL Server 6.5, 7.0, 2000, 2005, 2008, 2008R2 Sybase ASE/IQ 12.x, 15 MySQL V4, V5 PostgreSQL 7, 8, 8.4 Symfoware Server V7, V8, V9, V10
対応DBMSの プラットフォーム	上記DBMSが稼働する各社のUNIX Linux Microsoft Windows
Chakra 動作プラットフォーム	CPU　：Xeon 3GHz 2CPU相当以上、またはXeon 2.5GHz/4core相当以上 メモリー　：4GB以上を推奨 DISK　：保存するログデータ量に依存します。 OS　：Windows2000 / 2003 / 2008 Server / 2008 R2 Red Hat Enterprise Linux 3 / 4 / 5 CentOS 5 Network　：Ethernet Adapterを2枚以上

製品アライアンス

ORACLE　Symfoware　MySQL　asteria warp　JP1 CERTIFIED　Systemwalker Enabled　WebSAM

RSA enVision powerd by Express5800　ログレビ　Logstorage　splunk>　Log Auditor

LogStare　Waha! Transformer　監査ポータル　AUDIT MASTER　SecureCube Access Check

アライアンスパートナー

INTEC　Infoscience　infoteria　Aqua Systems.inc　日本電子公証機構 Digital Notarization Authority　ORACLE　FUJITSU

NEC　NRI SECURE TECHNOLOGIES　BeaconIT Empower Your Data　Networld　siteROCK

国内総販売代理店

NST New System Technology

株式会社ニューシステムテクノロジー

〒105-0004 東京都港区新橋2-12-17 新橋INビル7階
Tel 03-3597-0031　Fax 03-3597-0032
Email : info@kknst.com　http://www.kknst.com

販売パートナー